# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/FR05/000158

International filing date: 24 January 2005 (24.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0450129
Filing date: 23 January 2004 (23.01.2004)

Date of receipt at the International Bureau: 27 May 2005 (27.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 MAI 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITE

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

| | |
|---|---|
| DATE DE REMISE DES PIÈCES:<br>N° D'ENREGISTREMENT NATIONAL:<br>DÉPARTEMENT DE DÉPÔT:<br>DATE DE DÉPÔT: | Albert GRYNWALD<br>Cabinet GRYNWALD<br>127 rue du Faubourg Poissonnière<br>75009 PARIS<br>France |
| Vos références pour ce dossier: B11161 | |

| **1 NATURE DE LA DEMANDE** | | | |
|---|---|---|---|
| Demande de brevet | | | |
| **2 TITRE DE L'INVENTION** | | | |
| | Procédé pour établir, à partir d'un jeu de grands nombres premiers, un jeu de clés destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message | | |
| **3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE** | Pays ou organisation | Date | N° |
| **4-1 DEMANDEUR** | | | |
| Nom | FRANCE TELECOM | | |
| Rue | 6 Place d'Alleray | | |
| Code postal et ville | 75015 PARIS | | |
| Pays | France | | |
| Nationalité | France | | |
| Forme juridique | Société anonyme | | |
| N° SIREN | 380 129 866 | | |
| **5A MANDATAIRE** | | | |
| Nom | GRYNWALD | | |
| Prénom | Albert | | |
| Qualité | CPI: 95-1001, Pas de pouvoir | | |
| Cabinet ou Société | Cabinet GRYNWALD | | |
| Rue | 127 rue du Faubourg Poissonnière | | |
| Code postal et ville | 75009 PARIS | | |
| N° de téléphone | 01 53 32 77 35 | | |
| N° de télécopie | 01 53 32 77 94 | | |
| Courrier électronique | cabinet.grynwald@wanadoo.fr | | |
| **6 DOCUMENTS ET FICHIERS JOINTS** | Fichier électronique | Pages | Détails |
| Texte du brevet | textebrevet.pdf | 35 | D 27, R 7, AB 1 |
| Dessins | dessins.pdf | 3 | page 3, figures 4, Abrégé: page 3, Fig.2 |
| Désignation d'inventeurs | | | |

| | | | | |
|---|---|---|---|---|
| **7 MODE DE PAIEMENT** | | | | |
| Mode de paiement | Prélèvement du compte courant | | | |
| Numéro du compte client | 3339 | | | |
| **8 RAPPORT DE RECHERCHE** | | | | |
| Etablissement immédiat | | | | |
| **9 REDEVANCES JOINTES** | Devise | Taux | Quantité | Montant à payer |
| 062 Dépôt | EURO | 0.00 | 1.00 | 0.00 |
| 063 Rapport de recherche (R.R.) | EURO | 320.00 | 1.00 | 320.00 |
| 068 Revendication à partir de la 11ème | EURO | 15.00 | 10.00 | 150.00 |
| Total à acquitter | EURO | | | 470.00 |

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, Cabinet Grynwald, A.Grynwald
Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0
Fonction
Mandataire agréé (Mandataire 1)

R E P U B L I Q U E F R A N C A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITE

### Réception électronique d'une soumission

Il est certifié par la présente qu'une demande de brevet (ou de certificat d'utilité) a été reçue par le biais du dépôt électronique sécurisé de l'INPI. Après réception, un numéro d'enregistrement et une date de réception ont été attribués automatiquement.

**Demande de brevet : X**
**Demande de CU :**

| | | |
|---|---|---|
| ***DATE DE RECEPTION*** | 23 janvier 2004 | |
| ***TYPE DE DEPOT*** | INPI (PARIS) - Dépôt électronique | **Dépôt en ligne: X**<br>**Dépôt sur support CD:** |
| ***N° D'ENREGISTREMENT NATIONAL ATTRIBUE PAR L'INPI*** | 0450129 | |
| **Vos références pour ce dossier** | B11161 | |

**DEMANDEUR**

| | |
|---|---|
| Nom ou dénomination sociale | FRANCE TELECOM |
| Nombre de demandeur(s) | 1 |
| Pays | FR |

**TITRE DE L'INVENTION**

Procédé pour établir, à partir d'un jeu de grands nombres premiers, un jeu de clés destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message

**DOCUMENTS ENVOYES**

| | | |
|---|---|---|
| package-data.xml | Requetefr.PDF | fee-sheet.xml |
| Design.PDF | ValidLog.PDF | textebrevet.pdf |
| FR-office-specific-info.xml | application-body.xml | request.xml |
| dessins.pdf | indication-bio-deposit.xml | |

**EFFECTUE PAR**

| | |
|---|---|
| Effectué par: | A.Grynwald |
| Date et heure de réception électronique: | 23 janvier 2004 16:46:11 |
| Empreinte officielle du dépôt | F2:32:F8:B8:CF:5E:B8:A7:A8:84:18:B0:94:02:D6:D8:D5:25:36:1C |

/ INPI PARIS, Section Dépôt /

SIEGE SOCIAL
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

**Procédé et système pour établir, à partir d'un jeu de grands nombres premiers, un jeu de clés destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message.**

## Préambule de la description

*Domaine concerné*

La présente invention concerne un procédé et un système pour établir, à partir d'un jeu de grands nombres premiers, un jeu de clés destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message.

*Exposé du problème*

Inventée en 1977, la technologie RSA offre des services de confidentialité et d'intégrité. Mais ce caractère universel a un prix en termes de performances. Inventée en 1999, la technologie GQ2 n'offre pas de service de confidentialité. Elle est dédiée aux services d'intégrité. En authentification et en signature, le mécanisme GQ2, flexible et ajustable par paramètres, est bien plus performant que le mécanisme RSA, par trop rigide.

Depuis l'invention de la technologie RSA, le problème de la factorisation des nombres entiers a fait l'objet d'intenses recherches. Le problème résiste toujours malgré de notables progrès résultant davantage de l'évolution de la puissance des ordinateurs que de l'évolution des algorithmes de factorisation. C'est à juste titre que les utilisateurs font confiance à la technologie RSA et donc, au problème de la factorisation.

Chaque instance RSA repose sur le problème de la factorisation d'un module, dénoté **n'**, produit de deux grands facteurs premiers distincts, dénotés $\mathbf{p_1}$ et $\mathbf{p_2}$.

$$\mathbf{n' = p_1 \times p_2} \quad \text{avec} \quad \mathbf{p_1 < p_2}$$

Outre un module **n'**, une clé RSA publique comprend un exposant **e**.

Chaque instance GQ2 repose également sur le problème de la factorisation d'un module, dénoté **n"**, produit de plusieurs grands facteurs premiers dont

deux au moins sont distincts, dénotés $\mathbf{p_1}$ à $\mathbf{p_f}$.

$$\mathbf{n''} = \mathbf{p_1} \times \ldots \mathbf{p_f} \quad \text{avec} \quad \mathbf{p_1} \leq \mathbf{p_2} \ldots \leq \mathbf{p_f} \quad \text{et} \quad \mathbf{p_1} < \mathbf{p_f}$$

Outre un module **n"**, une clé GQ2 publique comprend encore au moins un paramètre de sécurité $\mathbf{k} > 1$ et un ou plusieurs nombres de base $\mathbf{g_1}$ à $\mathbf{g_m} > 1$ dont le produit est inférieur aux grands facteurs premiers.

Chaque instance de la technologie GQ2 met en œuvre une ou plusieurs paires de nombres, à savoir un nombre public **G**, déduit du nombre de base **g**, et un nombre privé **Q** par paire, satisfaisant les deux critères suivants.

**Critère de validité d'un nombre de base GQ2** — Par définition, pour le paramètre de sécurité $\mathbf{k} > 1$, un nombre $\mathbf{g} > 1$ est « valide » comme nombre de base lorsque dans l'anneau des entiers mod **n**, le nombre public **G** admet des racines $2^k$-ièmes. Le nombre privé **Q** correspondant est l'une de ces racines $2^k$-ièmes ou son inverse mod **n**. La « paire de nombres GQ2 » **Q** et **G** vérifie une équation, directe ou inverse, régie par l'exposant $\mathbf{v} = 2^k$ et le module **n**.

$$\mathbf{G} \equiv \mathbf{Q^v} \bmod \mathbf{n} \qquad \text{ou} \qquad \mathbf{G} \times \mathbf{Q^v} \equiv 1 \bmod \mathbf{n}$$

**Critère d'équivalence d'un jeu de clés GQ2 avec le problème de la factorisation du module n** — Par définition, un jeu de clés GQ2 est « sûr » au sens cryptographique lorsque la connaissance d'un ou plusieurs nombres privés de $\mathbf{Q_1}$ à $\mathbf{Q_m}$ induit la connaissance d'une décomposition non-triviale du module **n**. Alors, prouver la connaissance de la clé privée GQ2 sans la révéler revient à prouver la connaissance d'une décomposition non-triviale du module **n** sans la révéler.

L'équivalence d'un jeu de clés GQ2 avec le problème de la factorisation du module **n** établit une preuve de la sécurité du protocole d'authentification GQ2.

Les clés GQ2 et leur gestion sont compatibles avec les clés RSA. Le même module **n** peut sans problème de sécurité être utilisé en RSA et en GQ2. Cette compatibilité tend à consolider la position hégémonique de la

technologie RSA en évitant le recours à des problèmes autres que celui de la factorisation lorsque les performances du mécanisme RSA laissent à désirer, par exemple, des dispositifs à capacité de calcul limitée comme une carte à puce, et des dispositifs saturés comme un serveur calculant un nombre élevé de signatures.

Ainsi en cas de saturation d'un serveur, deux stratégies sont possibles sans changer de jeu de clés RSA, c'est-à-dire, avec le même module **n**, produit de deux facteurs premiers $\mathbf{p_1}$ et $\mathbf{p_2}$ donnés.

Ou bien, multiplier le nombre de serveurs en conservant le mécanisme RSA de signature.

Ou bien, diviser la charge de travail en changeant de mécanisme, en passant de RSA en GQ2.

En version classique de GQ2, chaque nombre de base $\mathbf{g_i}$ fixe un nombre public $\mathbf{G_i} = \mathbf{g_i}^2$. Lorsque $\mathbf{p_1} - 1$ et $\mathbf{p_2} - 1$ sont divisibles par deux mais pas par quatre, soit environ un quart des modules RSA, la version classique de GQ2 assure systématiquement le critère de validité du nombre de base, c'est-à-dire, quel que soit le paramètre de sécurité **k**, le nombre de base $\mathbf{g_i}$ peut prendre toute valeur > 1.

Mais plus la puissance de deux divisant $\mathbf{p_1} - 1$ et / ou $\mathbf{p_2} - 1$ grandit, c'est-à-dire, plus $\mathbf{p_1}$ et / ou $\mathbf{p_2}$ se ramifient, plus il devient difficile de trouver des nombres de base en version classique de GQ2.

La présente invention définit alors autrement les nombres publics $\mathbf{G_1}$ à $\mathbf{G_m}$ en fonction des nombres de base $\mathbf{g_1}$ à $\mathbf{g_m}$.

*Art antérieur*

**Elever au carré dans le corps des entiers mod p**

Chaque grand nombre premier **p** est impair, c'est-à-dire, congru à 1 ou à 3 mod 4, avec autant en moyenne dans chaque catégorie. Chaque grand nombre premier congru à 1 mod 4 est congru à 1 ou à 5 mod 8, avec autant en moyenne dans chaque catégorie. Chaque grand nombre premier congru

à 1 mod 8 est congru à 1 ou à 9 mod 16, avec autant en moyenne dans chaque catégorie, et ainsi de suite. En moyenne, un grand nombre premier sur $2^{\mathbf{b}}$ est congru à $2^{\mathbf{b}}+1$ mod $2^{\mathbf{b+1}}$; alors l'expression $(\mathbf{p}-1)/2^{\mathbf{b}}$ est un nombre impair.

Considérons un nombre **a** positif et une suite définie par :

$$\{\mathbf{x}_1 = \mathbf{a} \bmod \mathbf{p};\ \text{pour } \mathbf{i} > 0,\ \mathbf{x}_{i+1} = \mathbf{a} + \mathbf{x}_i \bmod \mathbf{p}\}$$

Aucun des nombres suivants n'est nul : $\mathbf{x}_1 = \mathbf{a} \bmod \mathbf{p}$, $\mathbf{x}_2 = 2 \times \mathbf{a} \bmod \mathbf{p}$, ... $\mathbf{x}_{p-1} = (\mathbf{p}-1) \times \mathbf{a} \bmod \mathbf{p}$. Tous différents, ils forment une permutation des nombres de 1 à **p**–1. Le produit $\{1 \times 2 \times 3 \times \ldots (\mathbf{p}-1)\} = \{(\mathbf{p}-1)\ !\}$ est donc égal au produit $\{(\mathbf{a} \bmod \mathbf{p}) \times (2 \times \mathbf{a} \bmod \mathbf{p}) \times (3 \times \mathbf{a} \bmod \mathbf{p}) \times \ldots ((\mathbf{p}-1) \times \mathbf{a} \bmod \mathbf{p})\}$, c'est-à-dire, le nombre premier **p** divise le nombre $\{(\mathbf{a}^{\mathbf{p}-1}-1) \times (\mathbf{p}-1)\ !\}$. Or **p** ne divise pas le nombre $\{(\mathbf{p}-1)\ !\}$. Donc p divise $\mathbf{a}^{\mathbf{p}-1}-1$. C'est le petit théorème de Fermat qui s'énonce comme suit : « Soit **p** un nombre premier et **a** un entier non divisible par **p**, **p** divise $\mathbf{a}^{\mathbf{p}-1}-1$. »

Considérons un nombre **a** positif, inférieur à **p**, et une suite définie par ;

$$\{\mathbf{x}_1 = \mathbf{a};\ \text{pour } \mathbf{i} > 0,\ \mathbf{x}_{i+1} = \mathbf{a} \times \mathbf{x}_i \bmod \mathbf{p}\}$$

Par définition, le « rang » de **a** par rapport à **p** est la période de la suite (le plus petit nombre **n** positif tel que $\mathbf{x}_{n+1} = a$). Selon le petit théorème de Fermat, le rang est égal à ou divise **p**–1. Dans le corps des entiers mod **p**, si **p** est congru à $2^{\mathbf{b}}+1$ mod $2^{\mathbf{b+1}}$, il y a $(\mathbf{p}-1)/2^{\mathbf{b}}$ éléments de rang impair et $(2^{\mathbf{b}}-1)\times(\mathbf{p}-1)/2^{\mathbf{b}}$ éléments de rang pair. Tout élément de rang **p**–1, dénoté **w**, est « primitif » car la suite de ses puissances modulaires successives, c'est-à-dire, {pour **i** de 1 à **p**–1, $\mathbf{w}^{\mathbf{i}} \bmod \mathbf{p}$}, comprend tous les éléments non-nuls du corps.

Dans le corps des entiers mod **p**, la fonction « élever au carré » divise par deux le rang des éléments de rang pair et ne modifie pas le rang des éléments de rang impair. Elle se représente par un graphe orienté formé de cycles et de branches. La figure 1 illustre les quatre cas les plus simples et les plus fréquents : 1) **b** = 1, c'est-à-dire, $\mathbf{p} \equiv 3 \pmod 4$, 2) **b** = 2, c'est-à-

dire, $\mathbf{p} \equiv 5 \pmod 8$, 3) $\mathbf{b} = 3$, c'est-à-dire, $\mathbf{p} \equiv 9 \pmod{16}$, 4) $\mathbf{b} = 4$, c'est-à-dire, $\mathbf{p} \equiv 17 \pmod{32}$,

Tout élément de rang impair (les carrés 18 de la figure 1) est dans un cycle. Chaque cycle est constitué de tous les éléments de même rang impair. Pour chaque nombre **x** égal à ou divisant $(\mathbf{p}-1)/2^{\mathbf{b}}$, il y a un cycle de $\varphi(x)$ éléments de rang **x** où $\varphi(x)$ est le nombre de nombres positifs, inférieurs à **x** et premiers avec **x**.

La fonction « élever à la puissance $\mathbf{s} = (\mathbf{p}-1+2^{\mathbf{b}})/2^{\mathbf{b}+1}$ » convertit tout élément d'un cycle, c'est-à-dire, de rang impair, en sa racine carrée dans le cycle, c'est-à-dire, de même rang. En effet, $2 \times \mathbf{s} - 1 = (\mathbf{p}-1)/2^{\mathbf{b}}$.

Par définition, par rapport à un nombre premier **p**, on dit qu'un nombre **a**, non-multiple de **p**, est un « résidu quadratique » ou un « non-résidu quadratique » selon que l'équation $\mathbf{x}^2 \equiv \mathbf{a} \bmod \mathbf{p}$ a des solutions ou pas. Dans le corps des entiers mod **p**, $(\mathbf{p}-1)/2$ éléments sont des non-résidus quadratiques, à savoir les « éléments primitifs » définis précédemment, et $(\mathbf{p}-1)/2$ éléments sont des résidus quadratiques.

Tout élément de rang pair est dans une branche. Une branche est attachée à chaque élément de rang impair (les carrés 18 de la figure 1). Il y a $(\mathbf{p}-1)/2^{\mathbf{b}}$ branches, toutes semblables. Chaque nœud (les carrés 20 de la figure 1) est un résidu quadratique de rang pair. Chaque feuille (les ronds 22 de la figure 1) est un élément primitif (non-résidu quadratique). Chaque branche comprend $2^{\mathbf{b}}-1$ éléments dont $2^{\mathbf{b}-1}$ feuilles, soit une longueur **b**.

La fonction « élever à la puissance $(\mathbf{p}-1)/2^{\mathbf{b}}$ » convertit n'importe quel élément primitif **w** en un élément $\omega$ dont les puissances successives sont les $2^{\mathbf{b}}$ racines en **x** de l'équation $\mathbf{x}^{\mathbf{y}} \equiv 1 \bmod \mathbf{p}$ avec $\mathbf{y} = 2^{\mathbf{b}}$. L'ensemble de ces $2^{\mathbf{b}}$ racines, c'est-à-dire, {pour **i** de 1 à $2^{\mathbf{b}}$, $\omega^{\mathbf{i}} \bmod \mathbf{p}$}, forme un groupe multiplicatif connu sous le nom de "groupe de Sylow". Dans le graphe, c'est le point fixe 1 et la branche qui y est rattachée.

Dans le corps des entiers mod **p**, n'importe quel élément non-nul s'écrit de

manière unique comme le produit (et le quotient) d'une des $2^b$ racines en **x** de l'équation $x^y \equiv 1 \bmod p$ avec $y = 2^b$ par un élément de rang impair. La fonction « élever à la puissance $(p-1)/2^b$ » convertit tout élément non-nul, dénoté **a**, en la racine, dénotée $\alpha$, qui lui est ainsi associée de manière unique.

**Symboles de Legendre et de Jacobi**

Par définition, le « symbole de Legendre » d'un nombre **a** positif par rapport à un nombre **p** premier est égal à $a^{(p-1)/2} \bmod p$. Sa valeur est 0 pour les multiples de **p**. Pour les non-multiples de **p**, sa valeur est +1 ou –1 selon que l'équation $x^2 \equiv a \bmod p$ a des solutions ou pas, c'est-à-dire, selon que le nombre **a**, non-multiple de **p**, est un « résidu quadratique » ou un « non-résidu quadratique » par rapport à **p**.

Par définition, le « symbole de Jacobi » par rapport à un nombre composé **n** est le produit des symboles de Legendre par rapport à chaque facteur premier de **n**, en répétant les symboles de Legendre pour les facteurs premiers qui se répètent.

Si le symbole de Jacobi du nombre **a** par rapport au nombre **n** vaut –1, alors l'équation $x^2 \equiv a \bmod n$ n'a pas de solution. L'inverse n'est pas vrai.

Chacun de ces symboles peut se calculer efficacement sans exponentielle et sans les facteurs premiers, en utilisant la « loi de réciprocité quadratique ».

**Rappels sur la technologie RSA**

Chaque instance de la technologie RSA utilise un module **n**, produit de deux grands facteurs premiers distincts $p_1$ et $p_2$. Un nombre **e** est « valide » comme exposant RSA lorsqu'il est premier avec $p_1 - 1$ et $p_2 - 1$. C'est le « critère de validité de l'exposant RSA ».

La technologie RSA est « asymétrique » en ce sens qu'elle met en œuvre une « paire de clés ». Une clé RSA publique comprend un exposant et un module, couramment dénotés $\langle e, n \rangle$. Une clé RSA privée comprend un exposant et un module, couramment dénotés $\langle d, n \rangle$.

Lorsque l'exposant **e** est premier avec $\mathbf{p_j} - 1$, la fonction « élever à la puissance **e** mod $\mathbf{p_j}$ » ne change pas le rang des éléments. Les éléments (de rang impair) de chaque cycle de la fonction « élever au carré mod $\mathbf{p_j}$ » se retrouvent permutés dans un cycle de la fonction « élever à la puissance **e** mod $\mathbf{p_j}$ ». Chaque élément (de rang pair) de n'importe quelle branche attachée à un cycle de la fonction « élever au carré » se retrouve dans un cycle de la fonction « élever à la puissance **e** », déduit du cycle des éléments de rang impair par multiplication par l'une des $2^{bj}-1$ racines de rang pair en **x** de l'équation $x^y \equiv 1 \bmod pj$ avec $y = 2^{bj}$. En particulier, la branche de la fonction « élever au carré » attachée à l'unité se transforme en $2^{bj}-1$ points fixes de la fonction « élever à la puissance **e** ». Pour tout nombre $\mathbf{d_j}$ tel que $\mathbf{p_j} - 1$ divise $\mathbf{e} \times \mathbf{d_j} - 1$, la fonction « élever à la puissance $\mathbf{d_j}$ mod $\mathbf{p_j}$ » inverse la fonction « élever à la puissance **e** mod $\mathbf{p_j}$ ».

L'anneau des entiers mod **n** est le produit du corps des entiers mod $\mathbf{p_1}$ par le corps des entiers mod $\mathbf{p_2}$. La fonction « élever à la puissance **e** mod **n** » permute l'anneau des entiers mod **n**. C'est la permutation RSA. La permutation RSA s'inverse par une autre fonction puissance, la fonction « élever à la puissance **d** mod **n** ». Les nombres **e** et **d** sont liés. En effet, **d** est le plus petit nombre positif tel que $\mathbf{p_1} - 1$ et $\mathbf{p_2} - 1$ divisent $\mathbf{e} \times \mathbf{d} - 1$, c'est-à-dire, $\mathbf{e} \times \mathbf{d} - 1$ est un multiple du plus petit commun multiple de $\mathbf{p_1} - 1$ et $\mathbf{p_2} - 1$.

$$\mathbf{e} \times \mathbf{d} = 1 \bmod \mathrm{ppcm}(\mathbf{p_1} - 1, \mathbf{p_2} - 1)$$

Une clé RSA privée se représente encore par cinq nombres, à savoir des facteurs premiers $\mathbf{p_1}$ et $\mathbf{p_2}$, des exposants $\mathbf{d_1}$ et $\mathbf{d_2}$ ($\mathbf{d_j}$ est le nombre positif inférieur à $\mathbf{p_j}$ tel que $\mathbf{p_j} - 1$ divise $\mathbf{e} \times \mathbf{d_j} - 1$) et un reste chinois **Cr** (**Cr** est le nombre positif inférieur à $\mathbf{p_1}$ tel que $\mathbf{p_1}$ ($< \mathbf{p_2}$) divise $\mathbf{p_2} \times \mathbf{Cr} - 1$).

La représentation « chinoise » est la plus couramment utilisée. Pour inverser la permutation RSA, on calcule une composante $\mathbb{X}_j$ dans chaque corps en « élevant à la puissance $\mathbf{d_j}$ mod $\mathbf{p_j}$ ». Puis, on convertit les

composantes $X_1$ et $X_2$ en un résultat $X$ dans l'anneau des entiers mod $n$ en faisant appel au reste chinois.

$$z = Cr \times (X_1 - X_2) \bmod p_1 \qquad X = z \times p_2 + X_2$$

La technologie RSA offre des services d'intégrité et de confidentialité. L'exposant privé $d$ est, selon le service, utilisé pour signer ou pour déchiffrer. L'exposant public $e$ est, selon le service, utilisé pour vérifier ou pour chiffrer.

**Rappels sur la version classique de la technologie GQ2**

Outre un module $n$, produit de $f$ grands facteurs premiers $p_1$ à $p_f$ dont deux au moins sont distincts, chaque instance de la technologie GQ2 utilise un paramètre de sécurité $k > 1$ et un ou plusieurs nombres de base $g_1$ à $g_m$. Le paramètre de sécurité $k$ fixe un exposant $v = 2^k$. Chaque nombre de base $g_i > 1$ fixe un nombre public $G_i = g_i^2$. Chaque paire de nombres GQ2, à savoir un nombre public $G_i$ et un nombre privé $Q_i$, vérifie une équation, directe ou inverse, régie par l'exposant $v$ et le module $n$.

$$G_i \equiv Q_i^v \bmod n \qquad \text{ou} \qquad G_i \times Q_i^v \equiv 1 \bmod n$$

La technologie GQ2 est également « asymétrique ». Elle met en œuvre une « paire de clés ».

Une clé GQ2 publique classique comprend un paramètre de sécurité $k$, un ou plusieurs nombres de base $g_1$ à $g_m$, et un module $n$.

Une clé GQ2 privée classique comprend un paramètre de sécurité $k$, un ou plusieurs nombres privés $Q_1$ à $Q_m$, et un module $n$.

Outre un paramètre de sécurité $k$, une clé GQ2 privée classique se représente encore par $f \times (m+2) - 1$ nombres, à savoir des facteurs premiers $p_1$ à $p_f$, des restes chinois $Cr_1$ à $Cr_{f-1}$, et des composantes privées $Q_{1,1}$ à $Q_{m,f}$ (telles que $Q_{i,j} = Q_i \bmod p_j$). Cette représentation « chinoise » est la plus couramment utilisée.

**Protocole GQ2 classique**

Un défi $d$ comporte $k-1$ bits par nombre de base. Il se représente par $m$

nombres notés $\mathbf{d_1}$ à $\mathbf{d_m}$. Chaque nombre $\mathbf{d_i}$ comporte $\mathbf{k}$–1 bits, du bit de poids fort $\mathbf{d_{i,1}}$ au bit de poids faible $\mathbf{d_{i,k}}$.

Appelée « témoin GQ2 », une première structure de calcul utilise une clé GQ2 privée et la protège.

A chaque mise en œuvre, le témoin tire au hasard un aléa $\mathbf{r_j}$ par facteur premier $\mathbf{p_j}$.

Pour chaque facteur premier $\mathbf{p_j}$, le témoin effectue essentiellement $\mathbf{k}$ carrés successifs pour convertir chaque aléa $\mathbf{r_j}$ en une composante d'engagement $\mathbf{T_j}$.

$$T_j = r_j^{2^k} \bmod p_j \quad (1)$$

Puis, par composition chinoise, le témoin convertit les composantes $\mathbf{T_1}$ à $\mathbf{T_f}$ en engagement $\mathbf{T}$.

Pour chaque facteur premier $\mathbf{p_j}$, le témoin entrelace $\mathbf{k}$–1 opérations multiplicatives avec $\mathbf{k}$–2 carrés à partir de 1 comme nombre de départ. Pour **ii** de 1 à $\mathbf{k}$–1, la **ii-ième** opération multiplicative consiste, pour **i** de **1** à **m**, à multiplier ou pas le nombre courant par $\mathbf{Q_{i,j}}$ mod **n** selon que le bit $\mathbf{d_{i,ii}}$ vaut 1 ou 0. Enfin, par une ultime multiplication par l'aléa $\mathbf{r_j}$, le témoin obtient la composante de réponse $\mathbf{D_j}$. Puis, il efface l'aléa $\mathbf{r_j}$. Le témoin effectue en tout $\mathbf{k}$–2 carrés et en moyenne ($\mathbf{k}$–1) × **m** / 2 multiplications.

$$D_j = r_j \times \prod_{i=1}^{m} Q_{i,j}^{d_i} \bmod p_j \quad (2)$$

Puis, par composition chinoise, le témoin convertit les composantes $\mathbf{D_1}$ à $\mathbf{D_f}$ en réponse **D**.

Appelée « contrôleur GQ2 », une autre structure de calcul dispose d'une clé GQ2 publique.

Le contrôleur rétablit un engagement **T'** à partir de n'importe quelle réponse **D** et de n'importe quel défi **d**. Il entrelace **k** carrés avec **k**–**1** opérations élémentaires. Pour **ii** de **1** à **k**–1, la **ii-ième** opération élémentaire suit le **ii-ième** carré; elle consiste, pour **i** de **1** à **m**, à multiplier ou pas mod **n** le résultat courant par $\mathbf{g_i}$ selon que le bit $\mathbf{d_{i,ii}}$ vaut 1 ou 0.

$$T' = D^v \times \prod_{i=1}^{m} G_i^{d_i} \bmod n \qquad (3)$$

Un « triplet GQ2 » comprend un engagement (un nombre **T** positif et inférieur à **n**), un défi (une chaîne **d** de **(k–1) × m** bits) et une réponse (un nombre **D** positif et inférieur à **n**), notés **{T, d, D}**.

Il y a deux modes de production de triplets GQ2.

« En mode privé », le témoin GQ2 produit des triplets GQ2 au hasard à partir de n'importe quel aléa positif et inférieur à **n**. Il calcule d'abord un engagement **T** selon une formule d'engagement (1), puis, une réponse **D** à n'importe quel défi **d** selon une formule de réponse (2).

« En mode public », le contrôleur GQ2 transforme n'importe quelle réponse **D** et n'importe quel défi **d** en un engagement **T** selon une formule de contrôle (3). N'importe qui peut ainsi produire des triplets GQ2 au hasard. Etant donné un ensemble de triplets produits au hasard, on ne sait pas en distinguer le mode de production, public ou privé, avec une probabilité sensiblement différente de une chance sur deux. Si les aléas et les réponses sont de rang impair, alors l'ensemble des triplets GQ2 forme une famille de **d** permutations (le défi **d** indice les permutations) de l'ensemble des éléments de rang impair de l'anneau des entiers mod **n**.

Flexible et ajustable aux besoins de l'application, le protocole peut se répéter en parallèle ou en série. Un paramètre de répétition **t** complète le paramètre de sécurité **k** et le paramètre de multiplicité **m**. Le produit **(k–1) × m × t** prend une valeur typique de 1 à 40 pour authentifier et de 80 ou plus pour signer.

Pour authentifier un message **M**, on émet le code de hachage **h(T || M)** au lieu de l'engagement **T**.

Pour signer un message **M**, au lieu de tirer le défi **d** au hasard, on utilise **h(T || M)**.

Exemple de construction d'un jeu classique de clés GQ2 à équivalence évidente

Voici une construction de jeu de clés GQ2 classique. Les **m** nombres de base sont les **m** premiers nombres premiers, c'est-à-dire, $\mathbf{g_1} = 2$, $\mathbf{g_2} = 3$, $\mathbf{g_3} = 5$, $\mathbf{g_4} = 7$, $\mathbf{g_5} = 11$, $\mathbf{g_6} = 13$, $\mathbf{g_7} = 17$, $\mathbf{g_8} = 19$, et ainsi de suite. Les deux grands facteurs premiers sont congrus à 3 mod 4, et tels qu'il y a au moins un nombre de base $\mathbf{g_i}$ dont les symboles de Legendre par rapport à $\mathbf{p_1}$ et $\mathbf{p_2}$ sont différents, c'est-à-dire, $(\mathbf{g_i} \mid \mathbf{p_1}) = -(\mathbf{g_i} \mid \mathbf{p_2})$.

Au moins une des **m** premières conditions suivantes est remplie. 1) Un facteur premier est congru à 3 mod 8 et l'autre à 7 mod 8. 2) Un facteur premier est congru à 1 mod 3 et l'autre à 2 mod 3. 3) Un facteur premier est congru à ±1 mod 5 et l'autre à ±2 mod 5. 4) Un facteur premier est congru à {1, 2, 4} mod 7 et l'autre à {3, 5, 6} mod 7. 5) Un facteur premier est congru à {1, 3, 4, 5, 9} mod 11 et l'autre à {2, 6, 7, 8, 10} mod 11. 6) Un facteur premier est congru à {±1, ±3, ±4} mod 13 et l'autre à {±2, ±5, ±6} mod 13. Et ainsi de suite.

Comme $\mathbf{p_1}$ et $\mathbf{p_2}$ sont congrus à 3 mod 4, chaque nombre public $\mathbf{G_i} = \mathbf{g_i}^2$ est sur un cycle pour $\mathbf{p_1}$ et sur un cycle pour $\mathbf{p_2}$, c'est-à-dire que $\mathbf{G_i}$ est de rang impair dans les deux corps dont le produit forme l'anneau des entiers mod **n**. Alors, le critère de validité du nombre de base GQ2 est satisfait systématiquement. Quelles que soient les valeurs du paramètre de sécurité **k** et du nombre de base $\mathbf{g_i}$, il existe un nombre privé $\mathbf{Q_i}$. Une séquence de **k–1** carrés modulaires convertit le nombre $\mathbf{Q_i}$ en un nombre $\gamma_i$. Dans l'anneau des entiers mod **n**, le nombre $\gamma_i$ est un carré et le nombre $\Gamma_i = \gamma_i / \mathbf{g_i}$ ou $\gamma_i \times \mathbf{g_i}$ (selon que l'équation GQ2 est directe ou inverse) est une racine carrée de l'unité, c'est-à-dire, **n** divise $\Gamma_i^2 - 1$.

Il y a au moins un nombre de base **g** pour lequel les symboles de Legendre par rapport à $\mathbf{p_1}$ et $\mathbf{p_2}$ diffèrent, c'est-à-dire, $(\mathbf{g} \mid \mathbf{p_1}) = -(\mathbf{g} \mid \mathbf{p_2})$. Les symboles de Jacobi par rapport au module **n** sont $(\pm\mathbf{g} \mid \mathbf{n}) = -1$; ni **g** ni **–g** ne sont des carrés dans l'anneau des entiers mod **n**. Le nombre $\Gamma$ vaut –1 mod l'un des facteurs premiers et +1 mod l'autre. Alors qu'il divise $\Gamma^2 - 1$, le

module **n** ne divise ni Γ+1, ni Γ–1. Le nombre Γ est différent de ±1. C'est une racine carrée non-triviale de l'unité dans l'anneau. Le jeu de clés GQ2 est équivalent à la factorisation du module **n** parce que la connaissance du nombre privé **Q** induit la connaissance d'une décomposition non-triviale du module **n**, à savoir $\mathbf{n} = \text{pgcd}(\Gamma+1, \mathbf{n}) \times \text{pgcd}(\Gamma-1, \mathbf{n})$.

Si le module **n** est congru à 1 mod 4 et si le symbole de Jacobi d'au moins un nombre de base $\mathbf{g_i}$ par rapport à **n** vaut –1, c'est-à-dire, $(\mathbf{g_i} \mid n) = -1$, alors l'équivalence du jeu de clés GQ2 avec le problème de la factorisation du module **n** est « évidente ».

Au moins une des **m** premières conditions suivantes est remplie. 1) Le module est congru à 5 mod 8. 2) Le module est congru à 1 mod 4 et à 2 mod 3. 3) Le module est congru à 1 mod 4 et à ±2 mod 5. 4) Le module est congru à 1 mod 4 et à {3, 5, 6} mod 7. 5) Le module est congru à 1 mod 4 et à {2, 6, 7, 8, 10} mod 11. 6) Le module est congru à 1 mod 4 et à {±2, ±5, ±6} mod 13. 7) Le module est congru à 1 mod 4 et à {±3, ±5, ±6, ±7} mod 17. 8) Le module est congru à 1 mod 4 et à {2, 3, 8, 10, 12, 13, 14, 15, 18} mod 19. Et ainsi de suite.

Si l'authentification GQ2 réussit, il y a deux interprétations.

Ou bien avec une probabilité limitée à une chance sur le nombre total de défis possibles, le contrôleur a affaire à une entité qui a deviné le défi.

Ou bien avec la probabilité complémentaire, le contrôleur a affaire à un témoin qui connaît les nombres privés ce qui revient à connaître une décomposition non-triviale du module **n**.

Un observateur ne sait pas distinguer les deux situations suivantes, d'une part, un protocole honnête se déroulant entre un contrôleur et un témoin, et d'autre part, une interaction entre deux entités qui ont convenu à l'avance d'un défi ou d'une séquence de défis. L'interaction simulée ne révèle rien sur la factorisation du module **n** qui est le secret sous-jacent. Par conséquent, le protocole honnête ne révèle rien non plus.

*Solution*

Procédé

L'invention concerne un procédé pour établir un jeu de clés se présentant sous la forme de **m** couples de valeurs privées $Q_1$, $Q_2$, ... $Q_m$ et publiques $G_1$, $G_2$, ... $Gm$ ou de paramètre dérivés de composantes privées $Q_{i,j}$ des valeurs privées $Q_i$. Le jeu de clés est établi à partir :

- de **f** grands facteurs premiers $p_1$, $p_2$, ... $p_f$ de plusieurs centaines de bits, **f** est supérieur ou égal à 2, et/ou
- de **m** nombres de base entiers $g_1$, $g_2$, ... $g_m$.

Le jeu de clés est utilisé dans un protocole destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité, et/ou
- l'intégrité d'un message M associé à cette entité.

Le protocole met en œuvre un module public **n** constitué par le produit des **f** facteurs premiers $p_1$, $p_2$, ... $p_f$ et/ou les **f** facteurs premiers. Le module **n** et les valeurs privées et publiques sont liés par des relations du type :

$$G_i \times Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

**v** désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1.

Chaque valeur publique $G_i$ s'exprime sous la forme du $a_i$-**ième** carré du nombre de base $g_i$ , où $a_i$ désigne un paramètre d'ajustement du nombre de base $g_i$ par rapport au module **n** respectant la condition selon laquelle au moins un des paramètres d'ajustement $a_i$ est supérieur à 1.

Le procédé comprend les étapes suivantes :

- l'étape de déterminer le paramètre d'ajustement $a_i$ de telle sorte que chaque valeur publique $G_i$ soit de rang impair par rapport à chaque facteur premier $p_1$, $p_2$, ... $p_f$,
- l'étape de calculer les valeurs privées $Q_i$ ou les paramètres dérivés des

composantes privées $Q_{i,j}$ des valeurs privées $Q_i$ à partir des valeurs publiques $G_i$ ainsi déterminées.

De préférence, selon l'invention, le procédé est tel que le paramètre d'ajustement $a_i$ est le même pour tous les $g_i$.

De préférence, selon l'invention, le procédé est tel que le paramètre d'ajustement $a_i$ est égal à une valeur entière $c_i$ relative au nombre de base $g_i$. La valeur $c_i$ est la plus petite valeur entière telle que le $c_i$ - ième carré de $g_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$. La valeur entière $c_i$ est nulle dans le cas où le nombre de base $g_i$ est de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$.

De préférence, selon l'invention, le procédé est tel que le paramètre d'ajustement $a_i$ est égal à une valeur entière $c$. La valeur $c$ est la plus petite valeur entière $c$ telle que le $c$ - ième carré de chaque $g_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$. La valeur entière $c$ est nulle dans le cas où chaque nombre de base $g_i$ est de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$.

De préférence, selon l'invention, le procédé est plus particulièrement conçu pour satisfaire à un critère d'équivalence. Le procédé comprend les étapes suivantes :

- l'étape d'associer directement ou indirectement à une combinaison multiplicative d'un ou plusieurs nombres de base $g_1, g_2, \ldots g_m$ un indicateur,
- l'étape de former une fonction de l'indicateur, notamment les valeurs des carrés successifs de l'indicateur dans l'anneau des entiers modulo le module public $n$, permettant de sélectionner une combinaison satisfaisant au critère d'équivalence.

On peut ainsi déterminer un jeu de clés satisfaisant au critère d'équivalence (i) à partir des nombres de base de la combinaison ainsi sélectionnée et/ou (ii) à partir d'un jeu de nombres de base comprend les nombres de bases de

la combinaison sélectionnée.

De préférence, selon l'invention, l'indicateur figurant parmi les $2^{b1+ \ldots +bf}$ racines en $\mathbf{x}$ de l'équation $\mathbf{x^y \equiv 1 \bmod n}$ avec $\mathbf{y} = 2^{\max(b1 \text{ à } bf)}$ où les longueurs $\mathbf{b_1, b_2, \ldots b_f}$ sont déterminées à partir de l'ensemble des **f** facteurs premiers $\mathbf{p_1, p_2, \ldots p_f}$ de telle sorte que $\mathbf{p_j - 1}$ soit un multiple de $2^{bj}$, mais pas un multiple de $2^{bj+1}$.

De préférence, selon l'invention, l'indicateur est déterminé à partir de composantes d'indicateur. Une composante d'indicateur est obtenue en élevant la combinaison multiplicative à la puissance $(\mathbf{p_j} - 1)/2^{bj}$ dans le corps des entiers modulo $\mathbf{p_j}$. A chaque combinaison multiplicative on peut ainsi associer un indicateur.

Selon une première variante préférée de l'invention, le procédé comprend l'étape de sélectionner un ensemble de **m** nombres premiers parmi les 54 premiers nombres premiers tel que l'ensemble satisfasse un critère d'équivalence.

Selon une seconde variante préférée de l'invention, le procédé comprend l'étape de sélectionner un ensemble composé des **m** premiers nombres premiers tel que l'ensemble satisfasse un critère d'équivalence.

Selon une troisième variante préférée de l'invention, le procédé comprend l'étape de sélectionner un ensemble de **m** nombres premiers parmi les 54 premiers nombres premiers.

**Système**

L'invention concerne également un système pour établir un jeu de clés se présentant sous la forme de **m** couples de valeurs privées $\mathbf{Q_1, Q_2, \ldots Q_m}$ et publiques $\mathbf{G_1, G_2, \ldots Gm}$ ou de paramètre dérivés de composantes privées $\mathbf{Q_{i,j}}$ des valeurs privées $\mathbf{Q_i}$. Le jeu de clés est établi à partir :

- de **f** grands facteurs premiers $\mathbf{p_1, p_2, \ldots p_f}$ de plusieurs centaines de bits, **f** est supérieur ou égal à 1, et/ou
- de **m** nombres de base entiers $\mathbf{g_1, g_2, \ldots g_m}$.

Le jeu de clés est utilisé dans un protocole destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité, et/ou
- l'intégrité d'un message **M** associé à cette entité.

Le protocole met en œuvre un module public **n** constitué par le produit des **f** facteurs premiers $p_1, p_2, \ldots p_f$ et/ou les **f** facteurs premiers. Le module **n** et les valeurs privées et publiques sont liés par des relations du type :

$$G_i . Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

**v** désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1. Chaque valeur publique $G_i$ s'exprime sous la forme du $a_i$-ième carré du nombre de base $g_i$, où $a_i$ désigne un paramètre d'ajustement du nombre de base $g_i$ par rapport au module **n** respectant la condition selon laquelle au moins un des paramètres d'ajustement $a_i$ est supérieur à 1.

Le système comprend :

- des premiers moyens de traitement informatique, se présentant notamment sous la forme d'un équipement informatique tel qu'un calculateur numérique et/ou un microprocesseur situé dans une carte à puce, pour déterminer le paramètre d'ajustement $a_i$ de telle sorte que chaque valeur publique $G_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$,
- des seconds moyens de traitement informatique, notamment les premiers moyens de traitement informatique, pour calculer les valeurs privées $Q_i$ ou les paramètres dérivés des composantes privées $Q_{i,j}$ des valeurs privées $Q_i$ à partir des valeurs publiques $G_i$ ainsi déterminées.

De préférence, selon l'invention, le système est tel que le paramètre d'ajustement $a_i$ est le même pour tous les $g_i$.

De préférence, selon l'invention, le système est tel que le paramètre

d'ajustement $\mathbf{a_i}$ est égal à une valeur entière $\mathbf{c_i}$ relative au nombre de base $\mathbf{g_i}$. La valeur entière $\mathbf{c_i}$ est nulle dans le cas où le nombre de base $\mathbf{g_i}$ est de rang impair par rapport à chaque facteur premier $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$. Le système comprend en outre :

- des troisièmes moyens de traitement informatique, notamment les premiers moyens de traitement informatique pour déterminer la plus petite valeur entière $\mathbf{c_i}$ telle que le $\mathbf{c_i}$ - ième carré de $\mathbf{g_i}$ soit de rang impair par rapport à chaque facteur premier $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$.

De préférence, selon l'invention, le système est tel que le paramètre d'ajustement $\mathbf{a_i}$ est égal à une valeur entière $\mathbf{c}$. La valeur entière $\mathbf{c}$ est nulle dans le cas où chaque nombre de base $\mathbf{g_i}$ est de rang impair par rapport à chaque facteur premier $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$. Le système comprend en outre :

- des troisièmes moyens de traitement informatique, notamment les premiers moyens de traitement informatique pour déterminer la plus petite valeur entière $\mathbf{c}$ telle que le $\mathbf{c}$ - ième carré de chaque $\mathbf{g_i}$ soit de rang impair par rapport à chaque facteur premier $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$.

De préférence, selon l'invention, le système est plus particulièrement conçu pour satisfaire à un critère d'équivalence. Le système comprend des quatrièmes moyens de traitement informatique, notamment les premiers moyens de traitement informatique :

- pour associer un indicateur, directement ou indirectement, à une combinaison multiplicative d'un ou plusieurs nombres de base $\mathbf{g_1}$, $\mathbf{g_2}$, ... $\mathbf{g_m}$,
- pour former une fonction de l'indicateur, notamment les valeurs des carrés successifs de l'indicateur dans l'anneau des entiers modulo le module public $\mathbf{n}$, permettant de sélectionner une combinaison satisfaisant au critère d'équivalence.

On peut ainsi déterminer un jeu de clés satisfaisant au critère d'équivalence (i) à partir des nombres de base de la combinaison ainsi sélectionnée et/ou (ii) à partir d'un jeu de nombres de base comprend les nombres de bases de

la combinaison sélectionnée.

De préférence, selon l'invention, l'indicateur figurant parmi les $2^{b1+ \ldots +bf}$ racines en **x** de l'équation $x^y \equiv 1 \bmod n$ avec $y = 2^{max(b1 \text{ à } bf)}$ où les longueurs $b_1, b_2, \ldots b_f$ sont déterminées à partir de l'ensemble des **f** facteurs premiers $p_1, p_2, \ldots p_f$ de telle sorte que $p_j - 1$ soit un multiple de $2^{bj}$, mais pas un multiple de $2^{bj+1}$.

De préférence, selon l'invention, les quatrièmes moyens de traitement informatique permettant de déterminer l'indicateur à partir de composantes d'indicateur obtenues en élevant la combinaison multiplicative à la puissance $(p_j - 1)/2^{bj}$ dans le corps des entiers modulo $p_j$,. Ainsi à chaque combinaison multiplicative on peut associer un indicateur.

Selon une première variante préférée de l'invention, le premier moyen de traitement informatique permettant de sélectionner un ensemble de **m** nombres premiers parmi les 54 premiers nombres premiers. L'ensemble satisfaisant un critère d'équivalence.

Selon une seconde variante préférée de l'invention, le premier moyen de traitement informatique permettant de sélectionner un ensemble composé des **m** premiers nombres premiers. L'ensemble satisfaisant un critère d'équivalence.

Selon une troisième variante préférée de l'invention, le premier moyen de traitement informatique permettant de sélectionner un ensemble de **m** nombres premiers parmi les 54 premiers nombres premiers.

**Description détaillée**

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et des figures ci-jointes sur lesquelles:

- la figure 1, déjà décrite, représente des graphes orientés relatifs à la fonction "élever au carré" dans le corps des entiers modulo **p**,
- la figure 2 illustre des nombres $g_i$, $G_i$ et la valeur $Q_{i,j}$ définis selon

une réalisation de l'invention,

- la figure 3 illustre l'ensemble des positions possibles pour une composante privée $\mathbf{Q_{i,j}}$ dans le graphe d'une fonction "élever au carré modulo $\mathbf{p_j}$", et
- la figure 4 est une vue schématique d'un système selon l'invention.

**Paramètre d'ajustement**

Rappelons que le module **n** est le produit de **f** grands facteurs premiers $\mathbf{p_1}$ à $\mathbf{p_f}$ dont au moins deux sont distincts. Dès lors qu'au moins un grand facteur premier de $\mathbf{p_1}$ à $\mathbf{p_f}$ est congru à 1 mod 4, la version classique de GQ2, c'est-à-dire, $\mathbf{G_i} = \mathbf{g_i}^2$, n'assure plus systématiquement le critère de validité du nombre de base GQ2. Notre solution au problème posé fait appel aux nombres suivants.

Pour chaque grand facteur premier $\mathbf{p_j}$, un nombre $\mathbf{b_j}$ est défini de sorte que $\mathbf{p_j} - 1$ est divisible $\mathbf{b_j}$ fois par 2, mais pas $\mathbf{b_j} + 1$ fois. En d'autres termes, le nombre $\mathbf{b_j}$ est le nombre de bits à zéro en poids faible de la représentation binaire du nombre $\mathbf{p_j} - 1$.

Dans l'anneau des entiers mod **n**, à toute combinaison multiplicative de nombres de base, on associe un nombre **z** figurant parmi les $2^{b1+\ \ldots\ +bf}$ racines en **x** de l'équation $x^y \equiv 1 \bmod n$ avec $y = 2^{\max(b1 \text{ à } bf)}$. Dans chaque corps des entiers mod $\mathbf{p_j}$, de $\mathbf{p_1}$ à $\mathbf{p_f}$, ce nombre **z** se présente en une composante $\mathbf{z_j}$ obtenue en appliquant la fonction « élever à la puissance $(\mathbf{p_j} - 1)/2^{bj} \bmod \mathbf{p_j}$ » à la combinaison.

Dans l'anneau des entiers mod **n**, la position du nombre de base $\mathbf{g_i}$ est un nombre $\mathbf{c_i}$ qui prend une valeur de 0 à $\mathbf{b} = \max(\mathbf{b_1} \text{ à } \mathbf{b_f})$. C'est le plus petit nombre tel que le $\mathbf{c_i}$-ième carré modulaire de $\mathbf{g_i}$ est de rang impair par rapport à chaque facteur premier $\mathbf{p_1}$ à $\mathbf{p_f}$, c'est-à-dire, 0 si c'est $\mathbf{g_i}$, 1 si c'est le carré de $\mathbf{g_i}$, 2 si c'est le deuxième carré de $\mathbf{g_i}$, et ainsi de suite, jusqu'à **b** si c'est le **b**-ième carré de $\mathbf{g_i}$. En d'autres termes, la position $\mathbf{c_i}$ est le rang

d'apparition de 1 dans la suite des carrés modulaires du nombre **z** associé au nombre de base $g_i$, c'est-à-dire, 0 si $z = 1$, 1 si $z^2 = 1$, 2 si $z^4 = 1$, jusqu'à **b** si le **b**-ième carré modulaire de **z** vaut 1.

Dans l'anneau des entiers mod **n**, la position d'ensemble des nombres de base $g_1$ à $g_m$ est la plus grande position de $c_1$ à $c_m$, dénotée **c**. Le nombre **c** est inférieur ou égal à $b = \max(b_1 \text{ à } b_f)$.

$c = \max(c_1, c_2, \ldots c_m)$

Pour satisfaire systématiquement le critère de validité du nombre de base, pour chaque nombre de base $g_i$, nous introduisons un « paramètre d'ajustement » dénoté $a_i$. Le nombre public $G_i$ est le $a_i$-ième carré du nombre de base $g_i$, de sorte que chaque nombre public $G_i$, de $G_1$ à $G_m$, soit de rang impair par rapport à chaque facteur premier, de $p_1$ à $p_f$.

$$G_i = g_i^{2^{e_i}}$$

Voici deux solutions que nous allons analyser très soigneusement.

La première solution utilise un paramètre d'ajustement par nombre de base. Pour le nombre de base $g_i$, la valeur minimum est la position spécifique $c_i$. Il n'y a pas d'intérêt à un paramètre d'ajustement $a_i$ supérieur ou égal à $c_i$. Le nombre public $G'_i$ est le nombre de base $g_i$ si $c_i$ est nul ou bien le $c_i$-ième carré de $g_i$ si $c_i$ est positif.

$$G'_i = g_i^{2^{e_i}}$$

La première solution se distingue de la solution classique dès lors qu'au moins un des nombres publics $G'_i$ n'est pas le carré du nombre de base $g_i$, c'est-à-dire, qu'au moins un des paramètres d'ajustement est différent de 1.

La seconde solution utilise le même paramètre d'ajustement pour l'ensemble des nombres de base. La valeur minimum est la position d'ensemble $c = \max(c_1, c_2, \ldots c_m)$. Il n'y a pas d'intérêt à un paramètre d'ajustement $a_i$ plus grand que **c**. Le nombre public $G''_i$ est le **c**-ième carré du nombre de base $g_i$.

$$G''_i = g_i^{2^c}$$

La seconde solution se distingue de la solution classique dès lors que le nombre **c** est plus grand que 1, ce qui implique qu'au moins un des grands facteurs premiers $\mathbf{p_1}$ à $\mathbf{p_f}$ est congru à 1 mod 4.

La figure 2 illustre les différents nombres $\mathbf{g_i}$, $\mathbf{G_i}$ et $\mathbf{Q_{i,j}}$ dans un corps avec $\mathbf{b_j} = 3$, c'est-à-dire, $\mathbf{p_j} \equiv 9 \bmod 16$, ainsi que $\mathbf{c_{i,j}} = 2$, et $\mathbf{a_i} = 3$.

Le nombre (((**k**–3)-ième carré de $\mathbf{Q_{i,j}}$) / ou × $\mathbf{g_i}$) est une racine carrée de –1.

Le nombre (((**k**–2)-ième carré de $\mathbf{Q_{i,j}}$) / ou × $\mathbf{g_i}^2$) est égal à –1.

Les nombres (((**k**–1)-ième carré de $\mathbf{Q_{i,j}}$) / ou × $\mathbf{g_i}^4$) et ($\mathbf{G_i}$ / ou × $\mathbf{g_i}^8$) sont tous les deux égaux à 1.

Le paramètre de sécurité **k** fixe un exposant $\mathbf{v} = \mathbf{2^k}$. Chaque facteur premier $\mathbf{p_j}$ détermine un nombre $\mathbf{u_j}$ égal au plus petit nombre positif tel que ($\mathbf{p_j}$ –1) / $2^{\mathbf{bj}}$ divise $\mathbf{v} \times \mathbf{u_j}$ –1 ou $\mathbf{v} \times \mathbf{u_j}$ +1 selon que l'équation GQ2 est directe ou inverse. Dans le corps des entiers mod $\mathbf{p_j}$, la fonction « élever à la puissance $\mathbf{u_j}$ » convertit chaque nombre public $\mathbf{G_i}$ (de rang impair) en sa racine **v**-ième de rang impair.

$$Q_{i,j}\,(\text{de rang impair}) = G_i^{u_j} \bmod p_j$$

Dans le graphe de la fonction « élever au carré mod $\mathbf{p_j}$ », la figure 3 illustre l'ensemble des positions de la composante privée $\mathbf{Q_{i,j}}$, c'est-à-dire, l'ensemble des racines $2^{\mathbf{k}}$-ièmes du nombre public $\mathbf{G_i}$ (de rang impair), à savoir, d'abord, la valeur de rang impair, puis, son produit par –1, puis, son produit par les deux racines carrées de –1, puis, son produit par les quatre racines quatrièmes de –1, et ainsi de suite.

Toutefois, sans perte de généralité, on peut limiter la valeur de chaque composante privée, de $\mathbf{Q_{1,1}}$ à $\mathbf{Q_{m,f}}$, à la valeur de rang impair dans le corps des entiers, de mod $\mathbf{p_1}$ à mod $\mathbf{p_f}$. L'implémentation la plus simple, c'est-à-dire, la meilleure, utilise seulement les valeurs de rang impair.

Le nombre public $\mathbf{G_i}$, c'est-à-dire, le $\mathbf{a_i}$-ième carré du nombre de base $\mathbf{g_i}$, et le nombre privé $\mathbf{Q_i}$, c'est-à-dire, le nombre obtenu par composition chinoise

des composantes privées $\mathbf{Q_{i,1}}$ à $\mathbf{Q_{i,f}}$, forment ensemble une paire de nombres. Chaque paire de nombres vérifie une équation GQ2, directe ou inverse, régie par l'exposant $\mathbf{v} = 2^{\mathbf{k}}$ et le module **n**.

$$\mathbf{G_i} \equiv \mathbf{Q_i}^{\mathbf{v}} \bmod \mathbf{n} \qquad \text{ou} \qquad \mathbf{G_i} \times \mathbf{Q_i}^{\mathbf{v}} \equiv 1 \bmod \mathbf{n}$$

Pour analyser l'équivalence du jeu de clés avec le problème de la factorisation, nous introduisons un « indicateur » et une fonction de l'indicateur permettant d'établir un critère pratique pour déterminer si une combinaison satisfait ou non le « critère d'équivalence » avec le problème de la factorisation du module.

Le critère absolu pour assurer l'équivalence consiste à vérifier que parmi toutes les combinaisons multiplicatives des nombres de base, de $\mathbf{g_1}$ à $\mathbf{g_m}$, il y a au moins une combinaison pour laquelle les carrés modulaires successifs du nombre **z** passent à +1 sans passer par –1. Alors, le prédécesseur de +1 est une racine carrée non-triviale de l'unité dans l'anneau, ce qui assure qu'une décomposition non-triviale du module **n** se déduit des nombres privés $\mathbf{Q_1}$ à $\mathbf{Q_m}$. Le nombre **z** fait alors figure « d'indicateur » et la valeur du prédécesseur de +1 est la « fonction de l'indicateur ».

Le critère "simplifié" consiste à vérifier que parmi les nombres de base $\mathbf{g_1}$ à $\mathbf{g_m}$, il y a au moins un nombre de base $\mathbf{g_i}$ pour lequel le $(\mathbf{c_i}–1)$-ième carré de $\mathbf{z_i}$ dans l'anneau ne vaut pas –1.

Pour un nombre de base $\mathbf{g_i}$ et deux facteurs premiers $\mathbf{p_1}$ et $\mathbf{p_2}$, le critère minimal est le suivant.

Si $\mathbf{b_1} = \mathbf{b_2}$, les symboles de Legendre sont différents, c'est-à-dire, $(\mathbf{g_i} \mid \mathbf{p_1}) = -(\mathbf{g_i} \mid \mathbf{p_2})$.

Si $\mathbf{b_1} > \mathbf{b_2}$, le symbole de Legendre par rapport à $\mathbf{p_1}$ vaut –1, c'est-à-dire, $(\mathbf{g_i} \mid \mathbf{p_1}) = -1$.

Si $\mathbf{b_1} < \mathbf{b_2}$, le symbole de Legendre par rapport à $\mathbf{p_2}$ vaut –1, c'est-à-dire, $(\mathbf{g_i} \mid \mathbf{p_2}) = -1$.

Le symbole de Legendre fait alors figure « d'indicateur » et les règles

précédentes font figure de « fonction de l'indicateur ».

Pour deux grands facteurs premiers produits au hasard, chacun des premiers nombres premiers a au moins une chance sur deux de satisfaire le critère absolu, et exactement une chance sur deux de satisfaire le critère minimal.

Il y a plusieurs stratégies possibles pour choisir les nombres de base. Voici trois exemples.

On peut examiner les 54 premiers nombres premiers sachant que le 54-ième est 251 (il y a 54 nombres premiers s'écrivant sur un octet) et en retenir m en minimisant la valeur maximum des positions de $\mathbf{c_1}$ **à** $\mathbf{c_m}$ tout en assurant le critère d'équivalence

On peut prendre systématiquement les **m** premiers nombres premiers comme nombres de base, c'est-à-dire, $\mathbf{g_1} = 2$, $\mathbf{g_2} = 3$, $\mathbf{g_3} = 5$, $\mathbf{g_4} = 7$, $\mathbf{g_5} = 11$, et ainsi de suite. Si le critère d'équivalence n'est pas rempli, on retire un nouveau jeu de grands facteurs premiers.

On peut prendre systématiquement les **m** premiers nombres premiers comme nombres de base, c'est-à-dire, $\mathbf{g_1} = 2$, $\mathbf{g_2} = 3$, $\mathbf{g_3} = 5$, $\mathbf{g_4} = 7$, $\mathbf{g_5} = 11$, et ainsi de suite. Même si certains jeux de clés GQ2 ne sont pas équivalents, le monde extérieur ne sait pas les distinguer. La proportion des jeux non-équivalents est alors bornée par $1/2^{\mathbf{m}}$, par exemple, moins d'un sur 65536 en prenant les seize premiers nombres premiers sachant que le seizième est 53 (il y a seize nombres premiers s'écrivant sur 6 bits ou moins).

Protocole de la première solution

Le défi comporte $\mathbf{k'} - \mathbf{c_i}$ bits pour le nombre de base $\mathbf{g_i}$. Pour que le protocole puisse utiliser chaque nombre de base $\mathbf{g_i}$, le paramètre de sécurité $\mathbf{k'}$ doit être plus grand que le paramètre d'ajustement $\mathbf{c_i}$, ce qui implique que le paramètre de sécurité $\mathbf{k'}$ doit être plus grand que **c**, le plus grand nombre de $\mathbf{c_1}$ à $\mathbf{c_m}$.

Au cœur du dispositif de calcul GQ2, un « témoin GQ2 » protège et utilise

une clé GQ2 privée. Selon cette première solution, une clé GQ2 privée comprend un paramètre de sécurité **k'**, des paramètres d'ajustement $\mathbf{c_1}$ à $\mathbf{c_m}$, des nombres privés $\mathbf{Q_1}$ à $\mathbf{Q_m}$, et un module **n**. Alternativement, en représentation « chinoise », outre un paramètre de sécurité et des paramètres d'ajustement, une clé GQ2 privée comprend des composantes privées $\mathbf{Q_{1,1}}$ à $\mathbf{Q_{m,f}}$, des facteurs premiers $\mathbf{p_1}$ à $\mathbf{p_f}$ et des restes chinois $\mathbf{Cr_1}$ à $\mathbf{Cr_{f-1}}$.

« En mode privé », le témoin GQ2 produit des triplets GQ2 au hasard, c'est-à-dire, à partir d'un aléa **r** ou de composantes d'aléas de $\mathbf{r_1}$ à $\mathbf{r_f}$, d'abord un engagement **T** (un nombre positif et inférieur à **n**) selon une formule d'engagement (4), puis, une réponse **D** (un nombre positif et inférieur à **n**) à n'importe quel défi **d** (une chaîne de $\mathbf{m \times k' - c_1 \ldots - c_m}$ bits) selon une formule de réponse. Ou bien (4).

$$T_1 = r_1^v \bmod p_1$$

$$T_2 = r_2^v \bmod p_2$$

$$\mathbf{z = Cr \times (T_1 - T_2) \bmod p_1} \quad \mathbf{T = z \times p_2 + T_2}$$

Ou bien (5)

$$T = r^v \bmod n$$

$$D_1 = r_1 \times \prod_{i=1}^{m} Q_{i,1}^{d_i} \bmod p_1$$

$$D_2 = r_2 \times \prod_{i=1}^{m} Q_{i,2}^{d_i} \bmod p_2$$

$$\mathbf{z = Cr \times (D_1 - D_2) \bmod p_1}$$

$$\mathbf{D = z \times p_2 + D_2}$$

Ou bien

$$D = r \times \prod_{i=1}^{m} Q_i^{d_i} \bmod n$$

A entropie de défi constante, la formule d'engagement (4) implique **c**–1 carrés de plus que GQ2 classique.

Un « contrôleur GQ2 » utilise une clé GQ2 publique. Selon cette première

solution, outre un module **n**, une clé GQ2 publique comprend un paramètre de sécurité **k'** et des nombres de base $\mathbf{g_1}$ à $\mathbf{g_m}$, chacun associé à une position $\mathbf{c_1}$ à $\mathbf{c_m}$.

« En mode public », le contrôleur GQ2 produit des triplets GQ2, c'est-à-dire, transforme n'importe quelle réponse **D** (un nombre positif et inférieur à **n**) et n'importe quel défi **d** (une chaîne de $\mathbf{m \times k' - c_1 \ldots - c_m}$ bits) en un engagement **T'** (un nombre positif et inférieur à **n**) selon une formule de contrôle (6).

$$T' = D^v \times \prod_{i=1}^{m} G_i^{d_i} \mod n \qquad (6)$$

La formule de contrôle (6) convertit la réponse **D** en un engagement rétabli **T'**. Le contrôleur commence par alterner des carrés avec des opérations élémentaires. La **j**-ième opération élémentaire suit le **j**-ième carré; pour **i** allant de 1 à **m**, le bit $\mathbf{d_{i,j}}$ indique si le résultat courant doit être multiplié ou pas par $\mathbf{g_i}$ mod **n**. A entropie de défi constante, la première solution implique **c**–1 carrés de plus que GQ2 classique.

Protocole de la seconde solution

Le défi comporte $\mathbf{k'' - c}$ bits par nombre de base. Pour que le protocole fonctionne, le paramètre de sécurité **k"** doit être plus grand que le paramètre d'ajustement **c**.

Au cœur du dispositif de calcul GQ2, un « témoin GQ2 » protège et utilise une clé GQ2 privée. Selon cette seconde solution, une clé GQ2 privée comprend un paramètre d'ajustement **c**, un paramètre de sécurité **k"** plus grand que **c**, des nombres privés $\mathbf{Q_1}$ à $\mathbf{Q_m}$ et un module **n**. Alternativement, en représentation « chinoise », outre le paramètre d'ajustement et le paramètre de sécurité, une clé GQ2 privée comprend des composantes privées $\mathbf{Q_{1,1}}$ à $\mathbf{Q_{m,f}}$, des facteurs premiers $\mathbf{p_1}$ à $\mathbf{p_f}$ et des restes chinois $\mathbf{Cr_1}$ à $\mathbf{Cr_{f-1}}$.

« En mode privé », le témoin GQ2 produit des triplets GQ2 au hasard, c'est-à-dire, à partir d'un aléa **r** ou de composantes d'aléas de $\mathbf{r_1}$ à $\mathbf{r_f}$, d'abord un engagement **T** (un nombre positif et inférieur à **n**) selon une formule d'engagement (7), puis, une réponse **D** (un nombre positif et inférieur à **n**) à n'importe quel défi **d** (une chaîne de $\mathbf{m} \times (\mathbf{k''}-\mathbf{c})$ bits) selon une formule de réponse (8).

$$T_1 = r_1^v \bmod p_1$$

$$T_2 = r_2^v \bmod p_2$$

puis,

$$\mathbf{z} = \mathbf{Cr} \times (\mathbf{T_1} - \mathbf{T_2}) \bmod \mathbf{p_1}$$

$$\mathbf{T} = \mathbf{z} \times \mathbf{p_2} + \mathbf{T_2} \qquad (7)$$

Ou bien

$$T = r^v \bmod n$$

$$D_1 = r_1 \times \prod_{i=1}^{m} Q_{i,1}^{d_i} \bmod p_1 \qquad D_2 = r_2 \times \prod_{i=1}^{m} Q_{i,2}^{d_i} \bmod p_2$$

$$\mathbf{z} = \mathbf{Cr} \times (\mathbf{D_1} - \mathbf{D_2}) \bmod \mathbf{p_1}$$

$$\mathbf{D} = \mathbf{z} \times \mathbf{p_2} + \mathbf{D_2} \qquad (8)$$

Ou bien

$$D = r \times \prod_{i=1}^{m} Q_i^{d_i} \bmod n$$

A entropie de défi constante, la formule d'engagement (8) implique **c**–1 carrés de plus que GQ2 classique.

Un « contrôleur GQ2 » utilise une clé GQ2 publique. Selon cette seconde solution, outre un module **n**, une clé GQ2 publique comprend un paramètre d'ajustement **c**, un paramètre de sécurité **k''** et un ou plusieurs nombres de base $\mathbf{g_1}$ à $\mathbf{g_m}$.

« En mode public », le contrôleur GQ2 produit des triplets GQ2, c'est-à-dire, transforme n'importe quelle réponse **D** (un nombre positif et inférieur à **n**) et n'importe quel défi **d** (une chaîne de $\mathbf{m} \times (\mathbf{k''}-\mathbf{c})$ bits) en un engagement **T'** (un nombre positif et inférieur à **n**) selon une formule de

contrôle (9).

$$T' = D^v \times \prod_{i=1}^{m} G_i^{d_i} \mod n$$

La formule de contrôle (9) convertit la réponse **D** en un engagement rétabli **T'**. Le contrôleur commence par alterner des carrés avec des opérations élémentaires. La **j**-ième opération élémentaire suit le **j**-ième carré; pour **i** allant de **1** à **m**, le bit $\mathbf{d_{i,j}}$ indique si le résultat courant doit être multiplié ou pas mod **n** par $\mathbf{g_i}$. A entropie de défi constante, la seconde solution implique **c**–1 carrés de plus que GQ2 classique.

## Revendications

**1.** Procédé pour établir un jeu de clés (1) se présentant sous la forme de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ ou de paramètre dérivés de composantes privées $Q_{i,j}$ des valeurs privées (2) $Q_i$ ;

ledit jeu de clés (1) étant établi à partir :

- de **f** grands facteurs premiers $p_1, p_2, \ldots p_f$ de plusieurs centaines de bits, **f** étant supérieur ou égal à 2, et/ou
- de **m** nombres de base entiers $g_1, g_2, \ldots g_m$ ;

ledit jeu de clés (1) étant utilisé dans un protocole destiné à prouver à une entité contrôleur (7),

- l'authenticité d'une entité (8), et/ou
- l'intégrité d'un message **M** associé à cette entité (8) ;

ledit protocole (5) mettant en œuvre un module public **n** constitué par le produit desdits **f** facteurs premiers (3) $p_1, p_2, \ldots p_f$ et/ou lesdits **f** facteurs premiers (3) ;

ledit module **n** et lesdites valeurs privées (2) et publiques étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

**v** désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

chaque valeur publique $G_i$ s'exprimant sous la forme du $a_i$-ième carré du nombre de base $g_i$ , où $a_i$ désigne un paramètre d'ajustement du nombre de base $g_i$ par rapport au module **n** respectant la condition selon laquelle au moins un desdits paramètres d'ajustement $a_i$ est supérieur à 1 ;

ledit procédé comprenant les étapes suivantes :

- l'étape de déterminer ledit paramètre d'ajustement $a_i$ de telle sorte que chaque valeur publique (10) $G_i$ soit de rang impair par rapport à chaque

facteur premier $p_1, p_2, \cdots p_f$,

- l'étape de calculer lesdites valeurs privées (2) $Q_i$ ou lesdits paramètres dérivés des composantes privées $Q_{i,j}$ des valeurs privées (2) $Q_i$ à partir des valeurs publiques $G_i$ ainsi déterminées.

**2.** Procédé selon la revendication 1 ; ledit procédé étant tel que ledit paramètre d'ajustement $a_i$ est le même pour tous les $g_i$.

**3.** Procédé selon la revendication 1 ; ledit procédé étant tel que ledit paramètre d'ajustement $a_i$ est égal à une valeur entière $c_i$ relative au nombre de base $g_i$ ; ladite valeur $c_i$ étant la plus petite valeur entière telle que le $c_i$ - ième carré de $g_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \cdots p_f$.

**4.** Procédé selon la revendication 1 ; ledit procédé étant tel que ledit paramètre d'ajustement $a_i$ est égal à une valeur entière $c$ ; ladite valeur $c$ étant la plus petite valeur entière $c$ telle que le $c$ - ième carré de chaque $g_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \cdots p_f$.

**5.** Procédé selon l'une quelconque des revendications 1 à 4 ; ledit procédé étant plus particulièrement conçu pour satisfaire à un critère d'équivalence ; ledit procédé comprenant les étapes suivantes :

- l'étape d'associer directement ou indirectement à une combinaison multiplicative d'un ou plusieurs nombres de base (4) $g_{1,}, g_{2,}, \cdots g_m$ un indicateur,

- l'étape de former une fonction dudit indicateur (15), notamment les valeurs des carrés successifs dudit indicateur (15) dans l'anneau des entiers modulo le module public n (9), permettant de sélectionner une combinaison satisfaisant au critère d'équivalence ;

de sorte que l'on peut déterminer un jeu de clés (1) satisfaisant au critère d'équivalence (i) à partir des nombres de base (4) de la combinaison ainsi sélectionnée et/ou (ii) à partir d'un jeu de nombres de base (4) comprenant les nombres de base (4) de la combinaison sélectionnée

**6.** Procédé selon la revendication 5 ; ledit indicateur (15) figurant parmi les $2^{b1+ \ldots +bf}$ racines en $x$ de l'équation $x^y \equiv 1 \bmod n$ avec $y = 2^{\max(b1 \text{ à } bf)}$ où les longueurs $\mathbf{b_1}$, $\mathbf{b_2}$, ... $\mathbf{b_f}$ sont déterminées à partir de l'ensemble des **f** facteurs premiers (3) $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ de telle sorte que $\mathbf{p_j} - 1$ soit un multiple de $\mathbf{2^{bj}}$, mais pas un multiple de $\mathbf{2^{bj+1}}$.

**7.** Procédé selon l'une quelconque des revendications 5 ou 6 ; ledit indicateur (15) étant déterminé à partir de composantes d'indicateur (15) ; une composante d'indicateur (15) étant obtenue en élevant ladite combinaison multiplicative (17) à la puissance $(p_j - 1)/2^{bj}$ dans le corps des entiers modulo $p_j$, ;

de sorte qu'à chaque combinaison multiplicative (17) on peut associer un indicateur (15).

**8.** Procédé selon l'une quelconque des revendications 1 à 7 ; ledit procédé comprenant l'étape de sélectionner un ensemble de m nombres premiers parmi les 54 premiers nombres premiers ; ledit ensemble satisfaisant un critère d'équivalence.

**9.** Procédé selon l'une quelconque des revendications 1 à 7 ;

ledit procédé comprenant l'étape de sélectionner un ensemble composé des m premiers nombres premiers ; ledit ensemble satisfaisant un critère d'équivalence.

**10.** Procédé selon l'une quelconque des revendications 1 à 7 ;

ledit procédé comprenant l'étape de sélectionner un ensemble de m nombres premiers parmi les 54 premiers nombres premiers.

**Système**

**11.** Système pour établir un jeu de clés (1) se présentant sous la forme de **m** couples de valeurs privées (2) $\mathbf{Q_1}$, $\mathbf{Q_2}$, ... $\mathbf{Q_m}$ et publiques $\mathbf{G_1}$, $\mathbf{G_2}$, ... $\mathbf{G_m}$ ou de paramètre dérivés de composantes privées $\mathbf{Q_{i,j}}$ des valeurs privées (2) $\mathbf{Q_i}$ ; ledit jeu de clés (1) étant établi à partir :

- de **f** grands facteurs premiers (3) $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ de plusieurs centaines de

bits, **f** étant supérieur ou égal à 1, et/ou

- de **m** nombres de base (4) entiers $g_1, g_2, \ldots g_m$ ;

ledit jeu de clés (1) étant utilisé dans un protocole (5) destiné à prouver à une entité contrôleur (7),

- l'authenticité d'une entité (8), et/ou
- l'intégrité d'un message **M** associé à cette entité (8) ;

ledit protocole (5) mettant en œuvre un module public **n** (9) (9) constitué par le produit desdits **f** facteurs premiers (3) $p_1, p_2, \ldots p_f$ et/ou lesdits **f** facteurs premiers (3) ;

ledit module **n** et lesdites valeurs privées (2) et publiques étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

**v** désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

chaque valeur publique (10) $G_i$ s'exprimant sous la forme du $a_i$-ième carré du nombre de base $g_i$ , où $a_i$ désigne un paramètre d'ajustement du nombre de base $g_i$ par rapport au module **n** respectant la condition selon laquelle au moins un desdits paramètres d'ajustement $a_i$ est supérieur à 1 ;

ledit système comprenant :

- des premiers moyens de traitement informatique (11), se présentant notamment sous la forme d'un équipement informatique tel qu'un calculateur numérique et/ou un microprocesseur situé dans une carte à puce, pour déterminer le paramètre d'ajustement $a_i$ de telle sorte que chaque valeur publique (10) $G_i$ soit de rang impair par rapport à chaque facteur premier $p_1, p_2, \ldots p_f$,
- des seconds moyens de traitement informatique (12), notamment lesdits premiers moyens de traitement informatique, pour calculer lesdites valeurs privées (2) $Q_i$ ou lesdits paramètres dérivés des composantes

privées $\mathbf{Q_{i,j}}$ des valeurs privées (2) $\mathbf{Q_i}$ à partir des valeurs publiques (10) $\mathbf{G_i}$ ainsi déterminées.

**12.** Système selon l'une des revendications 11 ou 12 ; ledit système étant tel que ledit paramètre d'ajustement $\mathbf{a_i}$ est le même pour tous les $\mathbf{g_i}$.

**13.** Système selon l'une des revendications 11 ou 12 ; ledit système étant tel que ledit paramètre d'ajustement $\mathbf{a_i}$ est égal à une valeur entière $\mathbf{c_i}$ relative au nombre de base $\mathbf{g_i}$ ;

ledit système comprenant en outre :

- des troisièmes moyens de traitement informatique (13), notamment lesdits premiers moyens de traitement informatique (11) pour déterminer la plus petite valeur entière $\mathbf{c_i}$ telle que le $\mathbf{c_i}$ - ième carré de $\mathbf{g_i}$ soit de rang impair par rapport à chaque facteur premier $\mathbf{p_1, p_2, \ldots p_f}$.

**14.** Système selon l'une des revendications 11 ou 12 ; ledit système étant tel que ledit paramètre d'ajustement $\mathbf{a_i}$ est égal à une valeur entière $\mathbf{c}$ ;

ledit système comprenant en outre :

- des troisièmes moyens de traitement informatique (13), notamment lesdits premiers moyens de traitement informatique (11) pour déterminer la plus petite valeur entière $\mathbf{c}$ telle que le $\mathbf{c}$ - ième carré de chaque $\mathbf{g_i}$ soit de rang impair par rapport à chaque facteur premier $\mathbf{p_1, p_2, \ldots p_f}$, .

**15.** Système selon l'une quelconque des revendications 11 à 14 ; ledit système étant plus particulièrement conçu pour satisfaire à un critère d'équivalence ;

ledit système comprenant des quatrièmes moyens de traitement informatique (14), notamment lesdits premiers moyens de traitement informatique (11) :

- pour associer un indicateur (15), directement ou indirectement, à une combinaison multiplicative (17) d'un ou plusieurs nombres de base (4) $\mathbf{g_{1,}}$, $\mathbf{g_{2,}} \ldots \mathbf{g_m}$ ,
- pour former une fonction dudit indicateur (15), notamment les valeurs des

carrés successifs dudit indicateur (15) dans l'anneau des entiers modulo le module public n (9), permettant de sélectionner une combinaison satisfaisant au critère d'équivalence ;

de sorte que l'on peut ainsi déterminer un jeu de clés (1) satisfaisant au critère d'équivalence (i) à partir des nombres de base (4) de la combinaison ainsi sélectionnée et/ou (ii) à partir d'un jeu de nombres de base (4) comprenant les nombres de base (4) de la combinaison sélectionnée.

**16.** Système selon la revendication 15 ; ledit indicateur (15) figurant parmi les $2^{b1+ \ldots +bf}$ racines en $x$ de l'équation $x^y \equiv 1 \bmod n$ avec $y = 2^{\max(b1 \text{ à } bf)}$ où les longueurs $\mathbf{b_1}$, $\mathbf{b_2}$, ... $\mathbf{b_f}$ sont déterminées à partir de l'ensemble des **f** facteurs premiers (3) $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ de telle sorte que $\mathbf{p_j} - 1$ soit un multiple de $\mathbf{2^{bj}}$, mais pas un multiple de $\mathbf{2^{bj+1}}$.

**17.** Système selon l'une quelconque des revendications 15 ou 16 ; lesdits quatrièmes moyens de traitement informatique (14) permettant de déterminer ledit indicateur (15) à partir de composantes d'indicateur (16) obtenues en élevant ladite combinaison multiplicative (17) à la puissance $(p_j - 1)/2^{bj}$ dans le corps des entiers modulo $p_j$, ;

de sorte qu'à chaque combinaison multiplicative (17) on peut associer un indicateur (15).

**18.** Système selon l'une quelconque des revendications 11 à 17 ; ledit premier moyen de traitement informatique (11) permettant de sélectionner un ensemble de m nombres premiers parmi les 54 premiers nombres premiers ; ledit ensemble satisfaisant un critère d'équivalence.

**19.** Système selon l'une quelconque des revendications 11 à 17 ; ledit premier moyen de traitement informatique (11) permettant de sélectionner un ensemble composé des m premiers nombres premiers ; ledit ensemble satisfaisant un critère d'équivalence.

**20.** Système selon l'une quelconque des revendications 11 à 17 ; ledit premier moyen de traitement informatique (11) permettant de sélectionner

un ensemble de m nombres premiers parmi les 54 premiers nombres premiers.

FIG_1

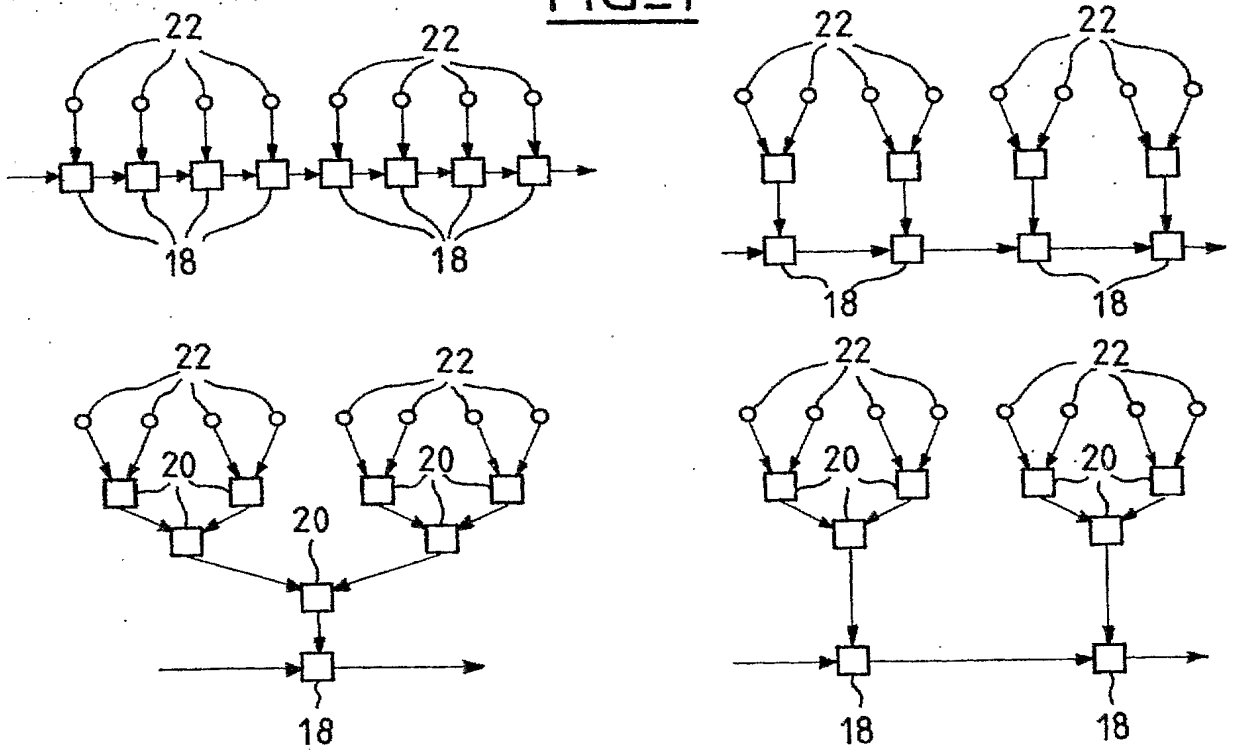



FIG_2

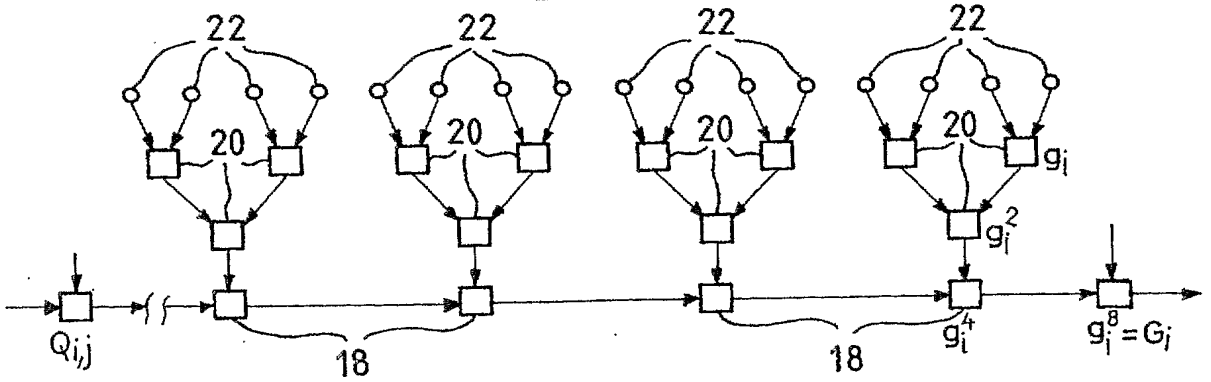
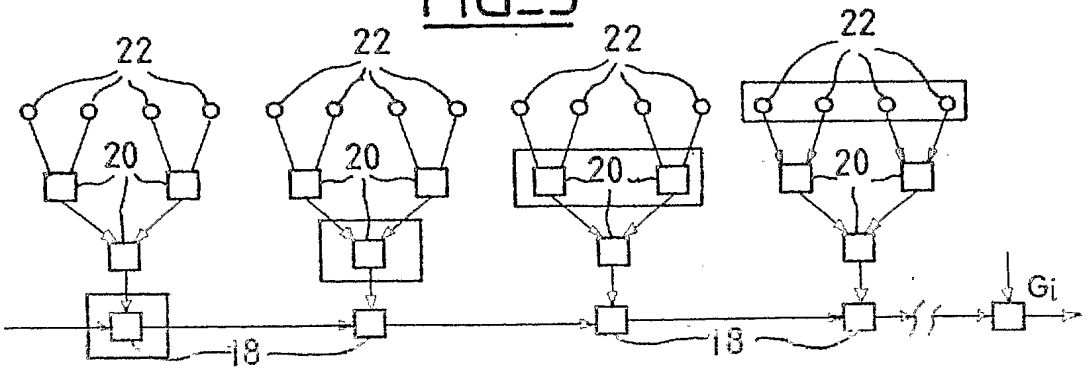



FIG_3



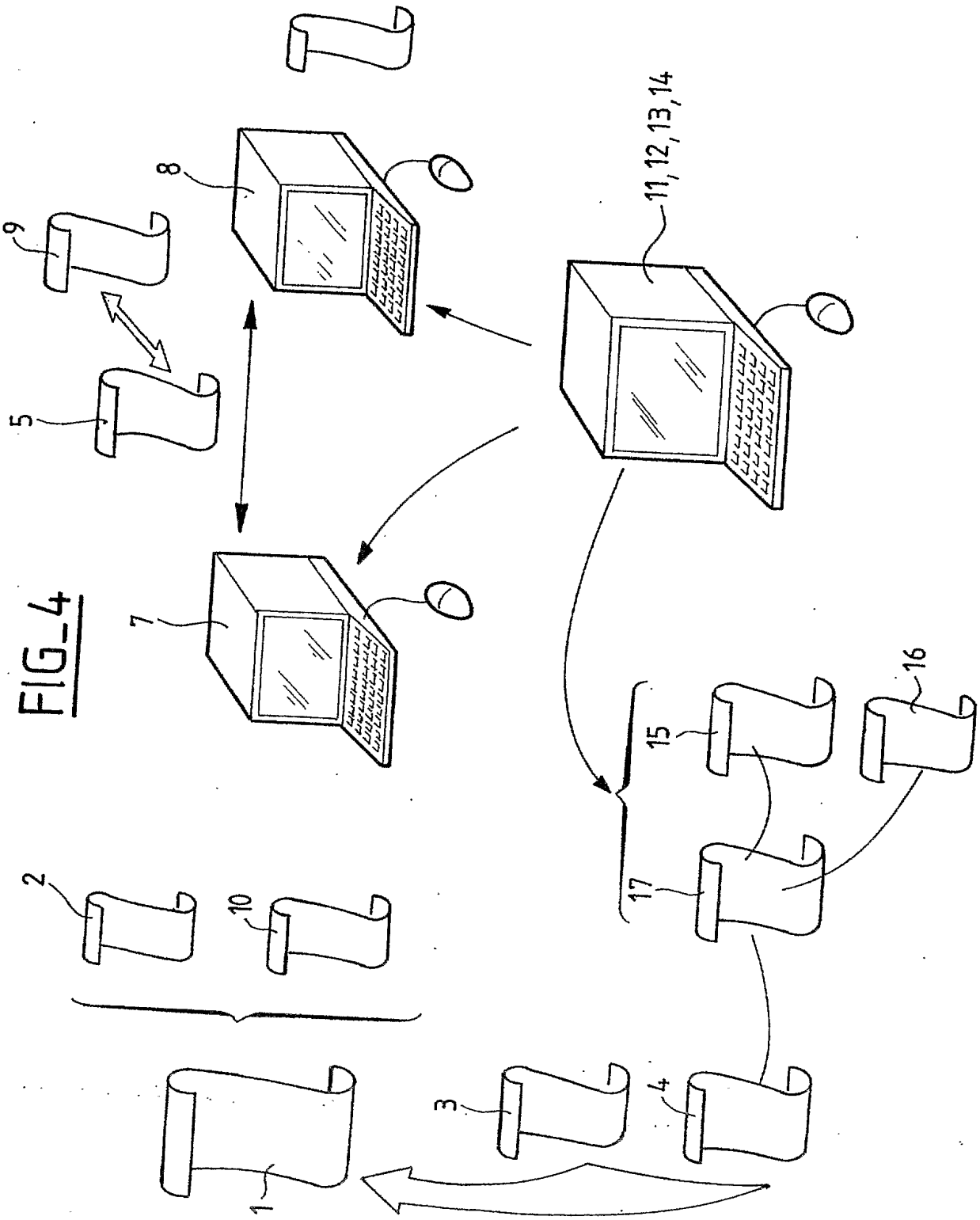



FIG_4

reçue le 24/02/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITE

## Désignation de l'inventeur

| | |
|---|---|
| **Vos références pour ce dossier** | B11161 |
| **N°D'ENREGISTREMENT NATIONAL** | |
| **TITRE DE L'INVENTION** | |
| | Procédé pour établir, à partir d'un jeu de grands nombres premiers, un jeu de clés destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message |
| **LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):** | |
| DESIGNE(NT) EN TANT QU'INVENTEUR(S): | |
| Inventeur 1 | |
| Nom | GUILLOU |
| Prénoms | Louis |
| Rue | 16 rue de l'Ise |
| Code postal et ville | 35230 BOURGBARRE |
| Société d'appartenance | |
| Inventeur 2 | |
| Nom | QUISQUATER |
| Prénoms | Jean-Jacques |
| Rue | 3 Avenue des Canards |
| Code postal et ville | B 1640 RHODE SAINT-GENESE |
| Société d'appartenance | |

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, Cabinet Grynwald, A.Grynwald
Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0
Fonction
Mandataire agréé (Mandataire 1)